AMENDMENT

In the Claims:

1. (Once Amended) A method for facilitating the delegation of operations involved in providing digital signatures to a signature server, the method comprising:

receiving a [request for a digital signature] message from a user at the signature server, the [request] message including an item to be signed on behalf of the user by the signature server;

looking up a private key for the user at the signature server; and

signing the item with the private key for the user[; and].

[returning the signed item to the user so that the user can send the signed item to a recipient.]

2. (Unchanged) The method of claim 1, wherein prior to signing the item, the method further comprises authenticating the user.

3. (Unchanged) The method of claim 2, wherein prior to signing the item, the method further comprises determining whether the user is authorized to sign the item.

4. (Unchanged) The method of claim 3, wherein determining whether the user is authorized to sign the item involves looking up an authorization for the user based upon an identifier for the user as well as an identifier for an application to which the user will send the signed item.

5. (Unchanged) The method of claim 3, wherein determining whether the user is authorized to sign the item involves communicating with an authority server that is separate from the signature server.

6. (Unchanged) The method of claim 1, further comprising allowing the user to authenticate the signature server prior to sending the [request] message to the signature server.

7. (Once Amended) The method of claim 1, further comprising returning the signed item to the user so that the user can send the signed item to a recipient. [facilitating encryption of communications between the user and the signature server.]

A1

8. (Unchanged) The method of claim 1, wherein the method further comprises configuring the signature server to accommodate a new user by:

receiving a request from an authorized entity to add the new user;

generating a key pair for the new user, including a new user private key and a new user public key;

communicating with a certification authority to obtain a certificate for the new user based on the key pair; and

storing the certificate and the key pair for the new user in a location that is accessible by the signature server to enable the signature server to sign items on behalf of the new user.

9. (Unchanged) The method of claim 1, wherein the method further comprises configuring the signature server to delete an old user by:

receiving a request from an authorized entity to delete the old user;

notifying a certification authority to revoke a certificate for the old user; and

removing the private key for the old user from the signature server, so that the signature server can no longer sign items on behalf of the old user.

10. (Once Amended) The method of claim 1, wherein the method further comprises archiving the [request] message and the signed item at the signature server.

11. (Unchanged) The method of claim 1, wherein the method further comprises forwarding the signed item to an archive server in order to be archived.

A1

12. (Once Amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for facilitating the delegation of operations involved in providing digital signatures to a signature server, the method comprising:

receiving a [request for a digital signature] message from a user at the signature server, the [request] message including an item to be signed on behalf of the user by the signature server;

looking up a private key for the user at the signature server; and

signing the item with the private key for the user[; and].

[returning the signed item to the user so that the user can send the signed item to a recipient.]

13. (Unchanged) The computer-readable storage medium of claim 12, wherein prior to signing the item, the method further comprises authenticating the user.

14. (Unchanged) The computer-readable storage medium of claim 13, wherein prior to signing the item, the method further comprises determining whether the user is authorized to sign the item.

15. (Unchanged) The computer-readable storage medium of claim 14, wherein determining whether the user is authorized to sign the item involves

looking up an authorization for the user based upon an identifier for the user as well as an identifier for an application to which the user will send the signed item.

16. (Unchanged) The computer-readable storage medium of claim 14, wherein determining whether the user is authorized to sign the item involves communicating with an authority server that is separate from the signature server.

17. (Once Amended) The computer-readable storage medium of claim 12, wherein the method further comprises allowing the user to authenticate the signature server prior to sending the [request] message to the signature server.

A1

18. (Once Amended) The computer-readable storage medium of claim 12, wherein the method further comprises returning the signed item to the user so that the user can send the signed item to a recipient. [facilitating encryption of communications between the user and the signature server.]

19. (Unchanged) The computer-readable storage medium of claim 12, wherein the method further comprises configuring the signature server to accommodate a new user by:

receiving a request from an authorized entity to add the new user;

generating a key pair for the new user, including a new user private key and a new user public key;

communicating with a certification authority to obtain a certificate for the new user based on the key pair; and

storing the certificate and the key pair for the new user in a location that is accessible by the signature server to enable the signature server to sign items on behalf of the new user.

20. (Unchanged) The computer-readable storage medium of claim 12, wherein the method further comprises configuring the signature server to delete an old user by:

receiving a request from an authorized entity to delete the old user;

notifying a certification authority to revoke a certificate for the old user; and

removing the private key for the old user from the signature server, so that the signature server can no longer sign items on behalf of the old user.

A1

21. (Once Amended) The computer-readable storage medium of claim 12, wherein the method further comprises archiving the [request] message and the signed item at the signature server.

22. (Unchanged) The computer-readable storage medium of claim 12, wherein the method further comprises forwarding the signed item to an archive server in order to be archived.

23. (Once Amended) An apparatus that facilitates delegating operations involved in providing digital signatures, comprising:

a signature server;

a receiving mechanism within the signature server that is configured to receive a [request for a digital signature] message from a user, the [request] message including an item to be signed on behalf of the user by the signature server;

a lookup mechanism within the signature server that is configured to look up a private key for the user; and

a signing mechanism within the signature server that is configured to sign the item with the private key for the user[; and].

[a sending mechanism within the signature server that is configured to return the signed item to the user so that the user can send the signed item to a recipient.]

24. (Unchanged) The apparatus of claim 23, further comprising an authentication mechanism that is configured to authenticate the user prior to signing the item.

25. (Unchanged) The apparatus of claim 24, further comprising an authorization mechanism that is configured to determine whether the user is authorized to sign the item prior to signing the item.

A1

26. (Unchanged) The apparatus of claim 25, wherein the authorization mechanism is configured to determine whether the user is authorized to sign the item by looking up an authorization for the user based upon an identifier for the user as well as an identifier for an application to which the user will send the signed item.

27. (Unchanged) The apparatus of claim 25, wherein the authorization mechanism is configured to determine whether the user is authorized to sign the item by communicating with an authority server that is separate from the signature server.

28. (Unchanged) The apparatus of claim 23, further comprising an authentication mechanism that is configured to allow the user to authenticate the signature server prior to sending the [request] message to the signature server.

29. (Once Amended) The apparatus of claim 23, further comprising a sending mechanism within the signature server that is configured to return the

signed item to the user so that the user can send the signed item to a recipient. [an encryption mechanism that is configured to facilitate encryption of communications between the user and the signature server.]

30. (Unchanged) The apparatus of claim 23, further comprising an initialization mechanism that is configured to:

receive a request from an authorized entity to add a new user;

generate a key pair for the new user, including a new user private key and a new user public key;

A1 communicate with a certification authority to obtain a certificate for the new user based on the key pair; and to

store the certificate and the key pair for the new user in a location that is accessible by the signature server to enable the signature server to sign items on behalf of the new user.

31. (Unchanged) The apparatus of claim 23, further comprising a deletion mechanism that is configured to:

receive a request from an authorized entity to delete an old user;

notify a certification authority to revoke a certificate for the old user; and to

remove the private key for the old user from the signature server, so that the signature server can no longer sign items on behalf of the old user.

32. (Once Amended) The apparatus of claim 23, further comprising an archiving mechanism that is configured to archive the [request] message and the signed item at the signature server.